NOTE ON THE DIRICHLET APPROXIMATION THEOREM

Yong-Cheol Kim

Abstract. We survey the classical results on the Dirichlet Approximation Theorem

In this chapter, we show up the theory of Diophantine approximation leads to understand how well real numbers can be captured by relations with the integers. In what follows, we denote by $\mathbb{N}_0 \fallingdotseq \mathbb{N} \cup \{0\}$.

Theorem 1.1 [Dirichlet's Approximation Theorem].
For each $\alpha \in \mathbb{R}$ and $N \in \mathbb{N}$, there are $n \in \mathbb{N}$ $(n \leq N)$ and $p \in \mathbb{Z}$ such that

$$\left|\alpha - \frac{p}{n}\right| < \frac{1}{Nn}, \quad i.e. \ |n\alpha - p| < \frac{1}{N}.$$

Proof. For $n \in \mathbb{N}_0$, we set $x_n = n\alpha - [n\alpha]$. We also divide $[0,1)$ into N half open subintervals of equal length

$$I_m = \left[\frac{m-1}{N}, \frac{m}{N}\right), \ m = 1, 2, \cdots, N.$$

Since $\{x_0, x_1, \cdots, x_N\} \subset \bigcup_{m=1}^{N} I_m$, at least two of x_n's belongs to a common interval I_{m_0}. Let x_k, x_ℓ be such two numbers inside I_{m_0} and let $k < \ell$. Then we have that

$$\frac{m_0 - 1}{N} \leq k\alpha - [k\alpha] < \frac{m_0}{N} \quad \text{and} \quad \frac{m_0 - 1}{N} \leq \ell\alpha - [\ell\alpha] < \frac{m_0}{N}.$$

By substracting those two inequalties, we obtain that

$$-\frac{1}{N} < \ell\alpha - k\alpha - ([\ell\alpha] - [k\alpha]) < \frac{1}{N}.$$

Then set $n = \ell - k \leq N$ and $p = [\ell\alpha] - [k\alpha]$. $\square$

Corollary 1.2 [Main theorem on the linear Diophantine equation].
For each $\dfrac{a}{b} \in \mathbb{Q}$ in lowest terms, there are $x, y \in \mathbb{Z}$ such that $ax - by = 1$.

Proof. If $b = 1$, then $ax - y = 1$ is solved by setting $x = 0$ and $y = -1$. Without loss of generality, we may assume that $b \geq 2$. Applying Theorem 1.1 with $N = b - 1$, there are $n \in \mathbb{N}$ $(n \leq N)$ and $p \in \mathbb{N}$ such that

$$|\alpha n - p| = \left|\frac{a}{b} n - p\right| < \frac{1}{N} = \frac{1}{b-1}.$$

Multiplying it by b leads to $|an - bp| < \dfrac{b}{b-1} = 1 + \dfrac{1}{b-1} \leq 2$. Since $an - bp \in \mathbb{Z}$, this implies that $|an - bp| \leq 1$.

The case that $an - bp = 0$ is excluded, since it implies that $\alpha = \frac{a}{b} = \frac{p}{n}$ and $n \le N = b - 1 < b$, which contradicts to the choice of $\frac{a}{b}$. Thus the only possibility is $an - bp = \pm 1$.

In case that $an - bp = 1$, we set $x = n$ and $y = p$; in case that $an - bp = -1$, we set $x = -n$ and $y = -p$. $\square$

Corollary 1.3. *The special Pell equation $x^2 - cy^2 = 1$ can be solved in the cases $c < 0$ and $c = a^2$ for $a \in \mathbb{Z}$.*

Proof. In case that $c = -1$ and $x^2 + y^2 = 1$, it can be solved by $x = \pm 1$, $y = 0$ or $x = 0$, $y = \pm 1$. In case that $c < -1$ and $x^2 + |c|y^2 = 1$, it can be solved by $x = \pm 1$, $y = 0$. Finally, in case that $c = a^2$ and $x^2 - cy^2 = (x - ay)(x + ay) = 1$, it can be solved by $x = \pm 1$, $y = 0$ for $a \neq 0$, or $x = \pm 1$, $y = t$ with $t \in \mathbb{Z}$ for $a = 0$. $\square$

Lemma 1.4. *For each $\alpha \in \mathbb{Q}^c$, there are infinitely many rationals $\frac{p}{n}$ in lowest terms such that*

$$\left|\alpha - \frac{p}{n}\right| < \frac{1}{n^2}.$$

Proof. Assume that there is a $\alpha_0 \in \mathbb{Q}^c$ such that

$$0 < \left|\alpha_0 - \frac{p_k}{n_k}\right| < \frac{1}{n_k^2} \quad \text{for all } k = 1, 2, \cdots, K.$$

Then we set $\delta = \min_{1 \le k \le K} \left[n_k \left|\alpha_0 - \frac{p_k}{n_k}\right| \right]$. Applying Theorem 1.1 with $N = \left[\frac{1}{\delta}\right] + 1 > \frac{1}{\delta}$, there are $n \in \mathbb{N}$ $(n \le N)$ and $p \in \mathbb{Z}$ such that

$$\left|\alpha_0 - \frac{p}{n}\right| < \frac{1}{nN}.$$

Without loss of generality, $\frac{p}{n}$ may here assumed to be in lowest terms. Then we have that

$$\left|\alpha_0 - \frac{p}{n}\right| \le \frac{1}{n^2},$$

and so $\frac{p}{n}$ is one of $\frac{p_k}{n_k}$'s. Thus, $p = p_k$ and $n = n_k$ for some $k, 1 \le k \le N$, and thus we obtain that

$$n_k \left|\alpha_0 - \frac{p_k}{n_k}\right| < \frac{1}{N} < \delta;$$

which contradicts to the definition of δ. $\square$

Corollary 1.5 [Fermat's theorem on the Pell equation].
If $c \in \mathbb{N}$ and $c \neq a^2$ for any $a \in \mathbb{Z}$, then the special Pell equation $x^2 - cy^2 = 1$ has infinitely many integral solutions.

Proof. First of all, we show that there is a single solution $x = \xi$, $y = \eta$ with $\eta \neq 0$. By Lemma 1.4, there are infinitely many rationals $\frac{p}{n}$ in lowest terms such that

$$0 < \left|\sqrt{c} - \frac{p}{n}\right| < \frac{1}{n^2}.$$

If we set $\alpha = p + n\sqrt{c}$ and $\overline{\alpha} = p - n\sqrt{c}$, then we have $|\overline{\alpha}| < \dfrac{1}{n}$, and so

$$|\alpha| = |p - n\sqrt{c} + 2n\sqrt{c}\,| \leq |\overline{\alpha}| + 2n\sqrt{c} \leq \frac{1}{n} + 2n\sqrt{c}.$$

Thus we have that $|p^2 - cn^2| = |\alpha\overline{\alpha}| \leq \left(\dfrac{1}{n} + 2n\sqrt{c}\right)\dfrac{1}{n} = \dfrac{1}{n^2} + 2\sqrt{c} \leq 2\sqrt{c} + 1$. Since the infinitely many integers $p^2 - cn^2$ lie in $[-2\sqrt{c} - 1, 2\sqrt{c} + 1]$, there is $a \in \mathbb{Z} \setminus \{0\}$ which coincides with infinitely many of the $p^2 - cn^2$. Set $\mathcal{F} = \{p + n\sqrt{c} : a = p^2 - cn^2\}$. Then we define the equivalence relation on $\mathcal{F}$ by

$$\alpha = p + n\sqrt{c} \sim \beta = q + m\sqrt{c} \;\Leftrightarrow\; p \equiv q,\, n \equiv m \;(\bmod\, |a|\,).$$

There are at most a^2 equivalence classes in the quotient space $\mathcal{F}/\sim$, and so in at least one of these finitely many equivalence classes there must be infinitely many of the numbers $\alpha, \beta, \cdots$ as above. Take such an equivalent pair $\alpha = p + n\sqrt{c}$, $\beta = q + m\sqrt{c}$ with $\alpha \neq \beta$; say, $|\alpha| > |\beta|$. So the number

$$\frac{\alpha - \beta}{a} = \frac{p - q}{a} + \frac{n - m}{a}\sqrt{c}$$

is of the form $x + y\sqrt{c}$, $x, y \in \mathbb{Z}$. Thus the number

$$\varepsilon \fallingdotseq \frac{\alpha}{\beta} = 1 + \frac{a}{b} \cdot \frac{\alpha - \beta}{a} = 1 + \frac{\beta\overline{\beta}}{\beta} \cdot \frac{\alpha - \beta}{a} = 1 + (q - m\sqrt{c})\left(\frac{p - q}{a} + \frac{n - m}{a}\sqrt{c}\right)$$

is of the form $\varepsilon = \xi + \eta\sqrt{c}$ with $\xi, \eta \in \mathbb{Z}$, for which

$$\xi^2 - c\eta^2 = \varepsilon\overline{\varepsilon} = \frac{\alpha\overline{\alpha}}{\beta\overline{\beta}} = \frac{a}{a} = 1.$$

Since $|\varepsilon| > 1$, we see that $\eta \neq 0$, and thus ξ, η is the required solution.

For the remaining part, we write $\varepsilon = \xi + \eta\sqrt{c}$ and $\overline{\varepsilon} = \xi - \eta\sqrt{c}$. Then we have that

$$1 = \xi^2 - c\eta^2 = (\xi + \eta\sqrt{c})(\xi - \eta\sqrt{c}) = \varepsilon \cdot \overline{\varepsilon},$$

and so $\varepsilon^n \cdot \overline{\varepsilon}^n = 1$ for all $n \in \mathbb{N}$. Moreover, the number $\varepsilon^n = (\xi + \eta\sqrt{c})^n$ is of the form $x + y\sqrt{c}$ with $x, y \in \mathbb{Z}$, which is represented uniquely by the irrationality of $\sqrt{c}$, and also $\varepsilon^n = x + y\sqrt{c}$ and $\overline{\varepsilon}^n = x - y\sqrt{c}$. Hence the infinitely many powers $\varepsilon^n = x + y\sqrt{c}$ lead to infinitely many solutions x, y of the special Pell equation, which are of course all distinct from each other since $|\varepsilon| \neq 1$. $\square$

Proposition 1.6. *$\alpha \in \mathbb{Q}^c$ if and only if for each $\varepsilon > 0$, there are $x, y \in \mathbb{Z}$ such that $0 < |\alpha x - y| < \varepsilon$.*

Proof. ($\Rightarrow$) By Lemma 1.4, there are infinitely many rationals $\dfrac{p_n}{q_n}$ with strictly increasing denominators satisfying $\left|\alpha - \dfrac{p_n}{q_n}\right| < \dfrac{1}{q_n^2}$. Given $\varepsilon > 0$, we choose $n \in \mathbb{N}$ so large that $q_n > \dfrac{1}{\varepsilon}$. Set $x = q_n$ and $y = p_n$. Then we have that $0 < |\alpha x - y| < \varepsilon$.

($\Leftarrow$) Assume that the righthand side holds. If $\alpha \in \mathbb{Q}$, i.e. $\alpha = \dfrac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then we have that

$$0 < \left|\frac{a}{b}x - y\right| < \frac{1}{b},$$

i.e. $0 < |ax - by| < 1$, which is impossible. $\square$

Example. *Set α equal to the Cantor series*

$$\alpha = \sum_{n=1}^{\infty} \frac{z_n}{g_1 g_2 \cdots g_n} = \frac{z_1}{g_1} + \frac{z_2}{g_1 g_2} + \frac{z_3}{g_1 g_2 g_3} + \cdots$$

with an increasing sequence of natural numbers $2 \le g_1 \le g_2 \le \cdots \le g_n \le \cdots$, $z_n \in \{0,1\}$, and $z_n = 1$ for infinitely many n. Then $\alpha \in \mathbb{Q}^c$ and the cardinal number of such α's is uncountable.

Proof. For $N \in \mathbb{N}$, we set $G_N = g_1 g_2 \cdots g_N$ and $\displaystyle\sum_{n=1}^{N} \frac{z_n}{g_1 g_2 \cdots g_n} = \frac{P_N}{G_N}$. Then we have that

$$\begin{aligned} 0 < \left|\alpha - \frac{P_N}{Q_N}\right| &= \left|\frac{z_{N+1}}{g_1 \cdots g_N\, g_{N+1}} + \frac{z_{N+2}}{g_1 \cdots g_N\, g_{N+1}\, g_{N+2}} + \cdots\right| \\ &\le \frac{1}{g_1 \cdots g_N\, g_{N+1}} \left(1 + \frac{1}{g_{N+2}} + \frac{1}{g_{N+2}\, g_{N+3}} + \cdots\right) \\ &\le \frac{1}{G_N\, g_{N+1}} \left(1 + \frac{1}{g_{N+1}} + \frac{1}{g_{N+1}^2} + \cdots\right) \\ &= \frac{1}{G_N g_{N+1}} \cdot \frac{1}{1 - \dfrac{1}{g_{N+1}}} = \frac{1}{G_N(g_{N+1} - 1)}. \end{aligned}$$

If the sequence $\{g_n\}$ is unbounded, then

$$0 < |\alpha G_N - P_N| \le \frac{1}{g_{N+1} - 1}$$

can be made to be arbitrarily small for all large enough N. So it follows from Proposition 1.6. □

Corollary 1.7. $e \in \mathbb{Q}^c$.

Proof. It easily follows from taking $g_n = n$ and $z_n = 1$ for all $n \in \mathbb{N}$ in the above example. □

Next we show up the irrationality of the second fundamental constant associated with the circle, i.e. π, $\zeta(2) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{6}\pi^2$, and $\zeta(3) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^3}$. The essential core of the proof is derived from the following formulae

$$\begin{aligned} \zeta(2) &= 1 + \frac{1}{2^2} + \cdots + \frac{1}{r^2} + \int_0^1 \int_0^1 \frac{(xy)^r}{1 - xy}\, dxdy, \\ \zeta(3) &= 1 + \frac{1}{2^3} + \cdots + \frac{1}{r^3} - \frac{1}{2} \int_0^1 \int_0^1 \frac{\ln(xy)}{1 - xy} (xy)^r\, dxdy. \end{aligned}$$

We obtain that for $r, s, \sigma \in \mathbb{N}_0$,

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1 - xy}\, dx\, dy = \sum_{k=0}^{\infty} \frac{1}{(k + r + \sigma + 1)(k + s + \sigma + 1)} \tag{1.1}$$

by expanding $(1 - xy)^{-1}$ as a geometric series. If $r = s$ and $\sigma = 0$ in (1.1), then we have that

$$\int_0^1 \int_0^1 \frac{(xy)^r}{1 - xy}\, dx\, dy = \zeta(2) - \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2}\right). \tag{1.2}$$

If $r > s$ in (1.1), then we have that

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1-xy}\, dx\, dy = \sum_{k=0}^{\infty} \left(\frac{1}{k+s+\sigma+1} - \frac{1}{k+r+\sigma+1} \right) \tag{1.3}$$
$$= \frac{1}{r-s} \left(\frac{1}{s+1+\sigma} + \cdots + \frac{1}{r+\sigma} \right),$$

which represents a rational number whose denominator is certainly given by $V(r)^2$, the square of the least common multiple $V(r)$ of $1, 2, \cdots, r$. Now we differentiate the both sides of (1.3) with respect to σ, and then set $\sigma = 0$. Then we obtain that

$$\int_0^1 \int_0^1 \frac{\ln(xy)}{1-xy}\, x^r y^s\, dx\, dy = \frac{-1}{r-s} \left(\frac{1}{(s+1)^2} + \cdots + \frac{1}{r^2} \right),\ r > s,$$

which describes a rational number whose denominator is certainly given by $V(r)^3$. We differentiate the both sides of (1.1) on the case $r = s$ with respect to σ, and then set $\sigma = 0$. Then we have that

$$\int_0^1 \int_0^1 \frac{\ln(xy)}{1-xy} (xy)^r\, dx\, dy = \sum_{k=0}^{\infty} \frac{-2}{(k+r+1)^3} \tag{1.4}$$
$$= -2 \left[\zeta(3) - \left(1 + \frac{1}{2^3} + \cdots + \frac{1}{r^3} \right) \right]$$

So it easily follows from (1.2) and (1.3) that

$$\int_0^1 \int_0^1 \frac{(1-y)^n P_n(x)}{1-xy}\, dx\, dy = \frac{a_n \zeta(2) + b_n}{V(n)^2}$$

where $P_n(x) = \frac{1}{n!} \left(\frac{d}{dx} \right)^n (x^n (1-x)^n)$ and a_n, b_n are some integers. Here we observe that $P_n(x)$ has only integral coefficients. Moreover, the integration by parts n-times with respect to x leads us to get

$$\frac{a_n \zeta(2) + b_n}{V(n)^2} = (-1)^n \int_0^1 \int_0^1 \frac{y^n (1-y)^n x^n (1-x)^n}{(1-xy)^{n+1}}\, dx\, dy.$$

Calculating the maximum value of the function $\frac{y(1-y)x(1-x)}{1-xy}$ on $[0,1] \times [0,1]$, we obtain that

$$0 \leq \frac{y(1-y)x(1-x)}{1-xy} \leq \left(\frac{\sqrt{5}-1}{2} \right)^5,$$

which implies that

$$\frac{|a_n \zeta(2) + b_n|}{V(n)^2} = \left| \int_0^1 \int_0^1 \frac{y^n (1-y)^n x^n (1-x)^n}{(1-xy)^{n+1}}\, dx\, dy \right|$$
$$\leq \left(\frac{\sqrt{5}-1}{2} \right)^{5n} \int_0^1 \int_0^1 \frac{1}{1-xy}\, dx\, dy \leq \left(\frac{\sqrt{5}-1}{2} \right)^{5n} \zeta(2).$$

Thus we obtain that

$$0 < |a_n \zeta(2) + b_n| \leq V(n)^2 \left(\frac{\sqrt{5}-1}{2} \right)^{5n} \zeta(2). \tag{1.5}$$

If we can show that $\lim_{n\to\infty} V(n)^2 \left(\frac{\sqrt{5}-1}{2}\right)^{5n} = 0$, we can apply Proposition 1.6 to conclude it because the righthand side of (1.5) could be chosen to be arbitrarily small. For this, we observe that $V(n) \le n^{\pi(n)}$ where $\pi(n)$ denotes the number of primes less than or equal to n. By the prime number theorem to be shown in Chapter 5, we see that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

Thus we have that $\pi(n) \le \ln 3 \cdot \frac{n}{\ln n}$, and so $V(n) \le n^{n^{\ln 3/\ln n}} = 3^n$ for all sufficiently large n. Hence we conclude that

$$0 \le \lim_{n\to\infty} V(n)^2 \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \le \lim_{n\to\infty} 9^n \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \le \lim_{n\to\infty} \left(\frac{5}{6}\right)^n = 0.$$

This proves Corollary 1.8 and Corollary 1.9.

Corollary 1.8. $\zeta(2) = \frac{1}{6}\pi^2 \in \mathbb{Q}^c$.

Corollary 1.9. $\pi \in \mathbb{Q}^c$.

Let us check up the irrationality of $\zeta(3)$. As in the above process, we obtain that

$$\int_0^1 \int_0^1 \frac{-\ln(xy)}{1-xy} P_n(x)\, P_n(y)\, dx\, dy = \frac{a_n\zeta(3)+b_n}{V(n)^3}$$

where a_n and b_n are some integers. The identity $\frac{-\ln(xy)}{1-xy} = \int_0^1 \frac{1}{1-(1-xy)z}\, dz$ leads to get that

$$\begin{aligned}
&\frac{a_n\zeta(3)+b_n}{V(n)^3}\\
&= \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x)\, P_n(y)}{1-(1-xy)z}\, dx\, dy\, dz\\
&= \int_0^1 \int_0^1 \int_0^1 \frac{(xyz)^n(1-x)^n\, P_n(y)}{(1-(1-xy)z)^{n+1}}\, dx\, dy\, dz \text{ (integration by parts n-times w.r.t. x)}\\
&= \int_0^1 \int_0^1 \int_0^1 (1-x)^n(1-w)^n \frac{P_n(y)}{1-(1-xy)w}\, dx\, dy\, dw \text{ (change of variable } w = \frac{1-z}{1-(1-xy)z} \text{)}\\
&= \int_0^1 \int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n w^n(1-w)^n}{(1-(1-xy)w)^{n+1}}\, dx\, dy\, dw \text{ (integration by parts n-times w.r.t. y).}
\end{aligned}$$

Computing the extreme value of the function $\frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w}$ on $[0,1]^3$, we have that

$$\frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w} \le (\sqrt{2}-1)^4.$$

Thus it follows from this and (1.4) that

$$\begin{aligned}
0 \le \frac{|a_n\zeta(3)+b_n|}{V(n)^3} &\le (\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 \int_0^1 \frac{1}{1-(1-xy)w}\, dx\, dy\, dw\\
&= (\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 \frac{-\ln(xy)}{1-xy}\, dx\, dy\\
&= 2\,\zeta(3) \cdot (\sqrt{2}-1)^{4n}.
\end{aligned}$$

Since $V(n) \le 3^n$ for all sufficiently large n, we have that

$$0 \le |a_n\zeta(3) + b_n| \le 2\,\zeta(3)\cdot 27^n \cdot (\sqrt{2}-1)^{4n} < 2\,\zeta(3)\left(\frac{4}{5}\right)^n \to 0 \ \text{ as } n \to \infty.$$

Hence this proves Corollary 1.10.

Corollary 1.10 [Apéry's Theorem]. $\zeta(3) = 1 + \dfrac{1}{2^3} + \dfrac{1}{3^3} + \dfrac{1}{4^3} + \cdots \in \mathbb{Q}^c$.

We next generalize the Dirichlet Approximation Theorem in Proposition 1.11 and Proposition 1.12. Moreover we prove its generalized formation containing them in Theorem 1.13 which is due to Kronecker.

Proposition 1.11. *For each $(\alpha_1, \cdots, \alpha_L) \in \mathbb{R}^L$ and $N \in \mathbb{N}$, there are $n \in \mathbb{N}$ $(n \le N^L)$ and $(p_1, \cdots, p_L) \in \mathbb{Z}^L$ such that*

$$\max_{1\le \ell \le L}\left|\alpha_\ell - \frac{p_\ell}{n}\right| < \frac{1}{Nn}.$$

Proposition 1.12 [due to Dirichlet]. *For each $(\alpha_1, \cdots, \alpha_L) \in \mathbb{R}^L$ and $N \in \mathbb{N}$, there are $p \in \mathbb{N}$ and $(n_1, \cdots, n_L) \in \mathbb{Z}^L \setminus \{0\}$ with $\max\limits_{1\le \ell\le L} |n_\ell| \le N^{1/L}$ such that*

$$\left|\sum_{\ell=1}^{L} \alpha_\ell n_\ell - p\right| < \frac{1}{N}.$$

Theorem 1.13 [Multidimensional Dirichlet Approximation Theoerm].
For each $(\alpha_{11}, \alpha_{12}, \cdots, \alpha_{ML}) \in \mathbb{R}^{ML}$ and $N \in \mathbb{N}$, there are $(p_1, \cdots, p_M) \in \mathbb{Z}^M$ and $(n_1, \cdots, n_L) \in \mathbb{Z}^L \setminus \{0\}$ with $\max\limits_{1\le\ell\le L} |n_\ell| \le N^{M/L}$ such that

$$\max_{1\le m\le M}\left|\sum_{\ell=1}^{L} \alpha_{m\ell} n_\ell - p_m\right| < \frac{1}{N}.$$

Proof. We observe that

$$\left(\ \sum_{\ell=1}^{L} \alpha_{1\ell}\, n_\ell - \left[\sum_{\ell=1}^{L} \alpha_{1\ell}\, n_\ell\right], \cdots, \sum_{\ell=1}^{L} \alpha_{M\ell}\, n_\ell - \left[\sum_{\ell=1}^{L} \alpha_{M\ell}\, n_\ell\right]\ \right) \in [0,1)^M. \tag{1.6}$$

We decompose $[0,1)^M$ into N^M subcubes

$$Q_{k_1,\cdots,k_M} = \left[\frac{k_1-1}{N}, \frac{k_1}{N}\right) \times \cdots \times \left[\frac{k_M-1}{N}, \frac{k_M}{N}\right),\ 1 \le k_m \le N.$$

If we fix $0 \le n_\ell \le P$, then there are $(P+1)^L$ L-tuples $(n_1, \cdots, n_L)$; moreover, the requirement for applying the Dirichlet pigeon hole principle is $(P+1)^L > N^M$, i.e. $P+1 > N^{M/L}$. Set $P = [N^{M/L}]$. By the pigeon hole principle, two of such M-tuples in (1.6) lie in one of the subcubes $Q_{k_1,\cdots,k_M}$; i.e. for all $m = 1, 2, \cdots, M$ and for distinct n'_ℓ and n''_ℓ,

$$\frac{k_m-1}{N} \le \sum_{\ell=1}^{L} \alpha_{m\ell}\, n'_\ell - \left[\sum_{\ell=1}^{L} \alpha_{m\ell}\, n'_\ell\right] < \frac{k_m}{N},$$
$$\frac{k_m-1}{N} \le \sum_{\ell=1}^{L} \alpha_{m\ell}\, n''_\ell - \left[\sum_{\ell=1}^{L} \alpha_{m\ell}\, n''_\ell\right] < \frac{k_m}{N}.$$

Set $n_\ell = n''_\ell - n'_\ell$ and $p_m = \left[\sum_{\ell=1}^{L} \alpha_{m\ell}\, n''_\ell\right] - \left[\sum_{\ell=1}^{L} \alpha_{m\ell}\, n'_\ell\right]$. Then we obtain that

$$\max_{1\le m\le M}\left|\sum_{\ell=1}^{L}\alpha_{m\ell}n_\ell - p_m\right| < \frac{1}{N}.$$

Since n'_ℓ, n''_ℓ are distinct and $0 \le n'_\ell, n''_\ell \le P \le N^{M/L}$, not all the n_ℓ are equal to zero and $\max_{1\le\ell\le L}|n_\ell| \le N^{M/L}$. $\square$

In the following corollary, one can ask how small linear forms $\left(\sum_{\ell=1}^{L}\alpha_{1\ell}\,x_\ell, \cdots, \sum_{\ell=1}^{L}\alpha_{M\ell}\,x_\ell\right)$ can occur.

Corollary 1.14. *Foe each $N \in \mathbb{N}$ and each M-tuples $\left(\sum_{\ell=1}^{L}\alpha_{1\ell}\,x_\ell, \cdots, \sum_{\ell=1}^{L}\alpha_{M\ell}\,x_\ell\right)$ of linear forms derived from $(\alpha_{m\ell}) \in \mathrm{Mat}_{M\times L}(\mathbb{R})$ $(M < L)$, there is $(x_1, \cdots, x_L) \in \mathbb{Z}^L\setminus\{0\}$ with $\max_{1\le\ell\le L}|x_\ell| \le N^{M/L}$ such that*

$$\max_{1\le m\le M}\left|\sum_{\ell=1}^{L}\alpha_{m\ell}\,x_\ell\right| \le 2\,L\cdot A\cdot N^{M/L-1}$$

where $A = \max_{1\le m\le M}|\alpha_{m\ell}|$.

Proof. By Theorem 1.13, there are $(p_1, \cdots, p_M) \in \mathbb{Z}^M$ and $(x_1, \cdots, x_L) \in \mathbb{Z}^L\setminus\{0\}$ with $\max_{1\le\ell\le L}|x_\ell| \le N^{M/L}$ such that

$$\max_{1\le m\le M}\left|\sum_{\ell=1}^{L}\kappa\,\alpha_{m\ell}\,x_\ell - p_m\right| < \frac{1}{N}.$$

We shall choose κ so that $\max_{1\le m\le M}|P_m| < 1$. Now we have that

$$|p_m| \le \left|p_m - \sum_{\ell=1}^{L}\kappa\,\alpha_{m\ell}\,x_\ell\right| + \kappa\left|\sum_{\ell=1}^{L}\alpha_{m\ell}\,x_\ell\right| < \frac{1}{N} + \kappa\sum_{\ell=1}^{L}|\alpha_{m\ell}|\cdot|x_\ell| \le \frac{1}{N} + \kappa\,L\cdot A\cdot N^{M/L}.$$

Setting $\frac{1}{N} + \kappa\,L\cdot A\cdot N^{M/L} = 1$, we obtain that $\kappa = \left(1 - \frac{1}{N}\right)\frac{1}{L\cdot A\cdot N^{M/L}}$ if $A > 0$; otherwise, it is trivial. Thus we conclude that for $N \ge 2$,

$$\left|\sum_{\ell}^{L}\alpha_{m\ell}\,x_\ell\right| < \frac{1}{\kappa N} = \frac{L\cdot A\cdot N^{M/L-1}}{1 - \frac{1}{N}} \le 2\,L\cdot A\cdot N^{M/L-1}.$$

If $N = 1$, then $|x_\ell| = 1$, and hence $\left|\sum_{\ell=1}^{L}\alpha_{m\ell}\,x_\ell\right| \le \sum_{\ell=1}^{L}|\alpha_{m\ell}| \le L\cdot A$. $\square$

Corollary 1.15 [Carl Ludwig Siegel's Lemma].

If the coefficients $a_{m\ell}$ of the M linear forms $\sum_{\ell=1}^{L}a_{m\ell}\,x_\ell$, $m = 1, 2, \cdots, M$, are integers and $M < L$, then there is $(x_1, \cdots, x_L) \in \mathbb{Z}^L \setminus \{0\}$ so that

$$\sum_{\ell=1}^{L}a_{1\ell}\,x_\ell = 0, \cdots, \sum_{\ell=1}^{L}a_{M\ell}\,x_\ell = 0.$$

Moreover, if $A = \max_{1 \le \ell \le L} \max_{1 \le m \le M} |a_{m\ell}|$, *then* $|x_\ell| \le \left(\left[(2\,L\,A)^{\frac{L}{L-M}} \right] + 1 \right)^{M/L}$.

Proof. Set $2\,L\,A\,N^{M/L-1} < 1$ in Corollary 1.14; i.e. $N > (2\,L\,A)^{L/(L-M)}$. Then we take $N = \left[(2\,L\,A)^{\frac{L}{L-M}} \right] + 1$. $\square$

References

1. G. M. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Science Publications.
2. Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag.